Administrative Procedure 311

SMART GLASSES, WEARBALE RECORDING DEVICES, AND AI ENABLED WEARABLE TECHNOLOGY

Purpose and Guiding Principles

Rapid developments in consumer technology have placed cameras, microphones, wireless connectivity, artificial intelligence, and cloud-based processing into devices that can look almost indistinguishable from ordinary eyewear, watches, earbuds, pendants, body worn cameras, and other everyday accessories.

Unlike a conventional smartphone, some wearable devices can capture photographs, video, audio, or other information from a first-person perspective without it being readily apparent to people nearby that recording or data processing is taking place. Some devices may also transmit information to third party servers where artificial intelligence can analyze images, recognize objects, transcribe conversations, translate speech, identify text, generate descriptions, or perform other automated functions.

The District recognizes that these technologies can provide legitimate educational and accessibility benefits. In particular, AI enabled smart glasses and similar technologies may assist students who are blind or visually impaired, students with disabilities, or students requiring other accommodations.

At the same time, covert or inappropriate recording can interfere with privacy, dignity, safety, academic integrity, and the school's responsibility to maintain a safe and respectful learning environment.

Information captured through wearable devices may also be copied, uploaded, analyzed, manipulated, or combined with other publicly available information. Images, voices, and video may potentially be used for impersonation, harassment, synthetic media, voice cloning, sexualized deepfakes, or other harmful purposes.

The purpose of this administrative procedure is to establish reasonable boundaries governing when and how wearable recording and AI enabled technologies may be used on school property and during school activities.

Scope

1. This policy applies to students, employees, volunteers, parents and caregivers, contractors, guests, and other visitors while:
    a) on school property;
    b) participating in school sponsored activities;
    c) attending school events where the school has supervisory responsibility;
    d) participating in field trips or extracurricular activities; or
    e) travelling on school provided or school arranged transportation.

2. This procedure applies regardless of whether a device is personally owned, school owned, borrowed, or supplied by a third party.

Devices Covered

3. For the purposes of this administrative procedure, a wearable recording or AI enabled device means a device worn or carried on the body that is capable of one or more of the following:
    a. taking photographs;
    b. recording video;
    c. recording or transmitting audio;
    d. live streaming;
    e. transmitting captured information to another device or online service;
    f. using artificial intelligence to analyze images, voices, text, surroundings, or individuals;
    g. performing facial, object, text, or environmental recognition;
    h. generating transcripts, summaries, descriptions, translations, or other AI generated outputs from information captured around the wearer.
4. Examples may include smart glasses, camera glasses, AI glasses, body worn cameras, camera equipped watches, wearable cameras, AI enabled pendants, and similar technologies, and may include a cellphone.
5. The presence of an AI feature is not required for this administrative procedure to apply. A pair of glasses containing only a camera or microphone, for example, remains a wearable recording device for the purposes of this administrative procedure.

General Principle: Possession Is Different From Use

6. The School distinguishes between possessing a device and activating its recording, transmission, or AI processing functions. Mere possession of a wearable device will not automatically constitute misconduct.
7. Students and other members of the school community must not use a wearable device to photograph, record, livestream, transmit, analyze, or otherwise capture another person's image, voice, activity, personal information, schoolwork, computer screen, conversation, or surroundings where doing so:
    a. violates this administrative procedures or another school policy;
    b. interferes with teaching or learning;
    c. compromises academic integrity;
    d. constitutes harassment, bullying, intimidation, or discrimination;
    e. creates a safety concern;
    f. infringes upon a reasonable expectation of privacy;
    g. involves sexualized or intimate content;
    h. circumvents school security or safeguarding procedures; or

i. is otherwise contrary to applicable law.

8. The fact that Canadian criminal law may permit a particular recording does not necessarily mean that the recording is permitted under school policy. Schools may establish reasonable rules governing conduct and technology use on its property or during school sponsored events, in order to maintain a safe, respectful, and effective learning environment.

Students

9. Students may not activate or use smart glasses or other wearable or hand held recording devices to photograph, video record, audio record, livestream, transmit, or AI-process people or activities at school unless:
    a. the use has been expressly authorized by a teacher or administrator for an educational purpose; or
    b. the device forms part of an approved disability related accommodation or individualized learning support.
10. Where a student brings such a device to school without authorization to use it, recording, transmission, and AI processing functions must remain disabled during instructional time and in other circumstances where school or district personal digital device rules require the device not to be used.
11. Where reasonably necessary, the School may require the device to be securely stored in accordance with established school procedures.

Recording Teachers, Staff, or Other Students

12. Students must not use wearable or handheld technology to covertly record teachers, staff members, students, visitors, classroom discussions, meetings, presentations, assessments, or private conversations contrary to school policy.
13. The District recognizes that Canadian law relating to recording conversations is more nuanced than a simple requirement that everyone being recorded must consent. This policy therefore establishes a school conduct expectation rather than representing that every unauthorized recording is necessarily illegal.
14. Unauthorized recording may nevertheless result in school-based consequences where it interferes with privacy, safety, respectful conduct, learning, or the operation of the school.

Accessibility and Disability Accommodation

15. Smart glasses and other wearable technologies can provide important accessibility functions, including reading printed text aloud, recognizing objects, describing surroundings, assisting with navigation, identifying colours, translating text, providing captions, and supporting communication.
16. Accordingly, the District will not impose a blanket prohibition where doing so would improperly interfere with a student's disability related needs.
17. Where wearable technology is required or proposed as an accommodation, documented in the student's Individualized Education Plan (IEP), the School will work collaboratively with the student, parent or caregiver where appropriate, relevant educational or accessibility

professionals, administration, and the School as well as the District Privacy Officer where necessary.

18. An accommodation plan should consider:
    a. what functions are required by the student;
    b. when and where the device needs to operate;
    c. whether continuous recording is necessary;
    d. whether photographs, video, or audio are stored;
    e. whether information is transmitted to cloud based services;
    f. what third parties receive or process information;
    g. applicable privacy and security requirements;
    h. whether less intrusive settings can provide the required accessibility function;
    i. how other student's and staff member's privacy can reasonably be protected; and
    j. how the accommodation can be implemented without stigmatizing the student.
19. An accommodation should be designed to meet the student's legitimate accessibility needs while minimizing unnecessary collection, retention, transmission, or disclosure of information about others.
20. The mere presence of a camera or AI system within an accessibility device is not, by itself, sufficient reason to deny an otherwise reasonable accommodation.

Staff

21. Employees must not use personally owned wearable or handheld recording or AI enabled devices to record students or collect student information in the course of their duties unless the use has been authorized in accordance with school or district policy.
22. School approved wearable technology may be used for legitimate educational purposes, including vocational instruction, accessibility, demonstrations, research activities, media production, or other approved learning activities.
23. Before technology that records or processes identifiable student information is formally adopted for educational use, the District should determine whether appropriate privacy, security, procurement, and information management reviews are required. Consideration should include:
    a. what information the device collects;
    b. why the information is necessary;
    c. where information is processed and stored;
    d. who has access to it;
    e. how long information is retained;
    f. whether information is used for advertising, profiling, analytics, or AI model training;
    g. whether the provider can use captured information for its own purposes;
    h. whether recordings can be deleted;

i. applicable contractual safeguards; and

j. whether a Privacy Impact Assessment or other privacy review is required.

24. Where recordings are created for legitimate educational purposes, they should be retained only for as long as required by applicable law, records management requirements, or the educational purpose for which they were collected.

Parents, Caregivers, Contractors, and Visitors

25. Parents, caregivers, contractors, volunteers, and visitors are expected to respect the privacy and dignity of students and staff while on school and District property.

26. The School and District may prohibit or restrict the use of wearable recording devices in classrooms, meetings, offices, counselling spaces, student support areas, and other locations where recording could interfere with privacy, safety, confidentiality, learning, or school operations.

27. Visitors may be required to deactivate recording, live streaming, or AI processing functionality while in restricted areas.

28. A school administrator may direct a visitor to stop using or remove an operational wearable recording device where its use is inconsistent with this policy or reasonably creates a privacy, safety, safeguarding, or operational concern.

29. A person who refuses to comply with a reasonable direction will be required to leave school property in accordance with applicable school district procedures and legal authority.

30. This section does not prohibit ordinary photography or recording at public school performances, sporting events, ceremonies, or similar events where such activity is otherwise permitted by the School. Separate restrictions may nevertheless apply to the publication, distribution, or subsequent misuse of those recordings.

High Privacy and High Risk Locations

31. Wearable and handheld recording devices must not be used to photograph, video record, livestream, or otherwise visually capture individuals in locations where there is a heightened expectation of privacy. These locations include:

a. washrooms;

b. toilet stalls;

c. changing rooms;

d. locker-room changing areas;

e. showers;

f. spaces being used for changing clothing;

g. medical examination or treatment areas where private care is being provided; and

h. other locations in which a person would reasonably expect a high degree of visual privacy.

31.1. **Additional restrictions apply in:**

a) Counselling and Student Support Areas

i) Recording is prohibited unless specifically authorized for a legitimate professional, accessibility, or safeguarding purpose.

b) Examinations and Assessments

i) Smart glasses and other wearable and handheld technologies capable of accessing, transmitting, recording, or generating information may be prohibited during examinations, tests, and assessments unless required under an approved accommodation.

Staff and Administrative Meetings

32. Recording must comply with applicable school or district policies and any lawful accommodation requirements.

Artificial Intelligence, Deepfakes, and Manipulated Media

33. Students and other members of the school community must not use photographs, video, audio, biometric characteristics, or other information captured at school to create harmful or deceptive AI generated or digitally manipulated representations of another person.
34. Prohibited conduct includes using another person's likeness, image, or voice for:
    a) sexualized or intimate deepfakes;
    b) so called "nudification;"
    c) sexualized face swapping;
    d) non-consensual synthetic intimate imagery;
    e) malicious impersonation;
    f) deceptive voice cloning;
    g) fabricated recordings intended to portray a person as saying or doing something they did not say or do;
    h) harassment, bullying, intimidation, extortion, or humiliation; or
    i) other conduct prohibited by school policy or law.
35. The School will assess the conduct and resulting harm, rather than simply the technology used.
36. AI generated material should not automatically be characterized as a criminal offence. Depending upon its nature and circumstances, however, synthetic or manipulated material may engage provisions of the Criminal Code or other applicable legislation and may warrant referral to law enforcement.

Sexualized Images, Voyeurism, and Child Sexual Abuse and Exploitation Material

37. The School treats any suspected creation, possession, distribution, or threatened distribution of sexualized imagery involving students or staff as a serious safeguarding matter.
38. Particular care must be taken where technology has been used to:
    a. surreptitiously record a person in circumstances involving a reasonable expectation of privacy;

b. record a person who is nude or engaged in sexual activity;

c. create or distribute intimate images without consent;

d. create sexualized AI generated representations depicting a person who is or appears to be under 18; or

e. possess, access, distribute, or make available material that may constitute child sexual abuse and exploitation material under Canadian law.

39. Where there are reasonable grounds to believe that material may constitute evidence of a criminal offence, staff should not unnecessarily view, copy, forward, download, screenshot, or distribute the material.

40. The matter must instead be handled under the School's safeguarding, critical incident, and law enforcement referral procedures.

Response to Suspected Violations

41. Where a staff member reasonably believes that a wearable device has been used contrary to this administrative procedure, the immediate priority is to stop any ongoing recording or transmission and protect students and staff from further harm.

42. Depending upon the circumstances, staff may:

    a. direct the person to stop recording or deactivate the device;

    b. separate the device from continued use in accordance with existing school or district policy;

    c. notify school administration;

    d. document what was observed or reported;

    e. preserve relevant information already lawfully available to the School;

    f. contact the School or District Privacy Officer where a privacy incident may have occurred;

    g. follow safeguarding or child protection procedures where appropriate; and

    h. contact law enforcement where there are reasonable grounds to believe a criminal offence may have occurred or where immediate safety concerns exist.

43. School employees should not conduct forensic searches of personal devices, attempt to defeat passwords, access private cloud accounts, or manipulate suspected evidence unless specifically authorized by law and applicable school or district procedures.

44. Where potential criminal evidence is involved, administrators will consider obtaining direction from law enforcement before accessing, deleting, resetting, searching, or otherwise manipulating the device.

Temporary Possession of a Device

45. Where existing school policy authorizes staff to temporarily take possession of a student's device, the device should be:

    a. handled only to the extent reasonably necessary;

b. securely stored;

c. documented where appropriate; and

d. returned in accordance with established school procedures unless another lawful process requires otherwise.

46. Staff should not promise that information on a device can be preserved, and staff should not attempt to electronically isolate, disable, unlock, search, or forensically preserve a device unless authorized under applicable procedures and law.

47. Nothing in this adminstrative procedure authorizes a search that would otherwise be unlawful.

Privacy Incidents Involving School Controlled Information

48. Where wearable or handheld technology used by the School, an employee, contractor, or service provider results in the unauthorized collection, use, disclosure, loss, or exposure of personal information under the School's custody or control, the incident must be reported promptly to the appropriate administrator and District Privacy Officer.

49. The School will respond in accordance with applicable privacy legislation, district privacy breach procedures, contractual obligations, and any notification requirements.

50. Where an AI or cloud provider is involved, the School should determine what information was transmitted, where it was transmitted, whether it was retained, whether it was accessible to third parties, and what steps are available to contain or delete the information.

Progressive and Proportionate Response

51. A violation of this policy will not automatically result in police involvement.

52. School responses should be proportionate to the student's age, maturity, circumstances, intent, previous conduct, nature of the recording, degree of harm, and any disability or other relevant individual circumstances. Responses may include:

    a. education and restorative intervention;

    b. temporary loss of device privileges;

    c. parent or caregiver involvement;

    d. administrative consequences consistent with the school's code of conduct;

    e. safeguarding intervention;

    f. privacy breach procedures;

    g. threat or risk assessment where appropriate; and

    h. referral to law enforcement or child protection authorities where circumstances reasonably warrant such involvement.

53. A student who inadvertently activates a device should not ordinarily be treated in the same manner as a student who deliberately records another person in a washroom or uses captured imagery to create sexualized synthetic content.

Education and Awareness

54. The District recognizes that an administrative procedure alone is insufficient.
55. Students, employees, and families should receive age appropriate information explaining:
    a. when recording is and is not permitted at school;
    b. why wearable cameras create different privacy considerations from conventional devices;
    c. the difference between Canadian recording law and school rules;
    d. consent and reasonable expectations of privacy;
    e. appropriate use of AI;
    f. risks associated with uploading another person's image or voice to AI platforms;
    g. deepfakes and synthetic media;
    h. academic integrity;
    i. accessibility and disability accommodation; and
    j. consequences associated with misuse.

Superintendent Approval Date: October 14, 2026

Legal References

- *Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165*
- *Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/2012*
- *School Act*
- *Human Rights Code*
- *Criminal Code*

Cross References

- *Access to Information and Protection of Privacy and Personal Information Policy*
- *Privacy Management Program*
- *Forms*

This administrative procedure will be interpreted and applied consistently with applicable Canadian and British Columbia law, including the School Act, the Freedom of Information and Protection of Privacy Act where applicable, the Human Rights Code, the Criminal Code, applicable Ministerial Orders and school district policies, and the school's obligations to accommodate students with disabilities. Should this administrative procedure conflicts with applicable legislation, a lawful accommodation, a court order, or binding school district policy, those requirements prevail**.**